

ABSTRACT OF THE INVENTION

Authentication functions are centralized in a security system to offload servers of this functionality, and to provide an end-to-end solution for secure internet transactions. The security system supports authentication functions for authenticating a server by requesting server certificates from a certificate authority, and sending server certificates to clients requesting authentication. The security system also authenticates clients by checking digital signatures, validating the client certificates, which includes checking CA signatures, checking the validity period of the signatures, maintaining a certificate revocation list (CRL), and checking client certificates against the CRL.